Удостоверяване на самоличност в две стъпки за web приложения чрез RFID и SMS

Калоян Миронов

Two-step Verification Using RFID and SMS: *The paper presents the needs of higher level security in the web applications. To avoid this problem, a method of verification using RFID cards and SMS messages was developed. In addition a J2EE application that provides the new method of verification was developed.*

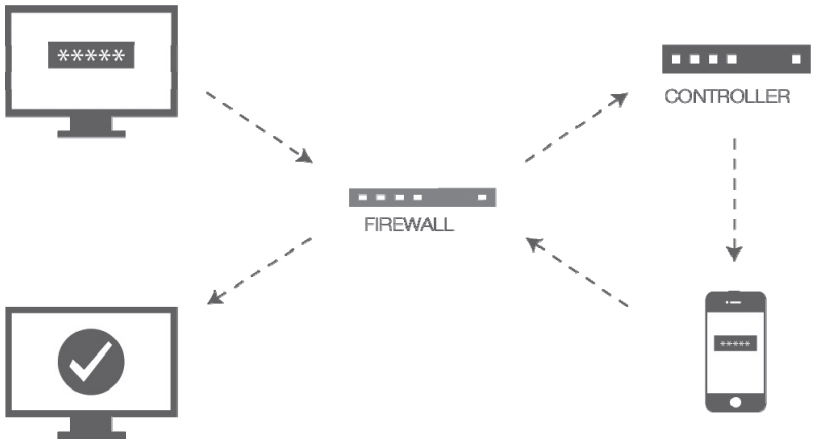
Key words: *2-step verification, web security, web-based application, RFID, SMS, J2EE.*

ВЪВЕДЕНИЕ

През последното десетилетие Web приложенията тенденциозно се налагат, като основен метод за обработка на информация и предоставяне на услуги, изместваики инсталационните програми. Фактори, като достъпност, интуитивно използване и липса на инсталация или конфигурация, правят web приложенията предпочитани пред останалите видове софтуер. Сигурността в Интернет винаги е била относително понятие. Методите за защита на информацията ни, както и тези за неправомерното й използване са две постоянно конкуриращи се величини. При разработването на нов метод за защита, рано или късно се появява злонамерен метод за преодоляване на съответната защита. За всяко web приложение е изключително важно да предостави на потребителите си защитена среда и неприкосновеност на личните данни. В тази статия ще представя метод за удостоверяване на самоличност при използване на web приложения. Методът се състои от две стъпки, което прави преодоляването му изключително трудно. Методът е използван при създаването на web приложение, реализиращо потвърждаване на самоличност.

УДОСТОВЕРЯВАНЕ На САМОЛИЧНОСТ В ДВЕ СТЪПКИ

Удостоверяването на самоличност в две или повече стъпки е подход за идентификация, при който се изисква представяне на два или повече фактора [1]. Факторите са независими един от друг и се определят, като: „нещо, което потребителят знае“ и „нещо, което притежава“. Типичен пример за този тип идентификация са факторите – парола (нещо, което потребителят знае) и код, получен чрез SMS (нещо, което притежава). На фигура 1 е представена последователността от процеси при този тип удостоверяване на самоличност.



Фигура 1. Модел на идентификация от две стъпки

От фигурата може да проследим, че след като потребителя въведе своята парола и тя бъде проверена, получава код на мобилния си телефон. За да завърши процеса по потвърждаване на самоличност се изисква кодът да бъде въведен. По този начин паролата, която сама по себе си е абстрактна и не носи информация за човека, който я въвежда, се асоциира с физически фактор, който показва принадлежност, а именно мобилният телефон на потребителя. Това прави този метод за удостоверяване на самоличност значително по-сигурен и предпочитан в системи, изискващи по-високо ниво на защита.

Използване на RFID и SMS за удостоверяване на самоличност

При внедряване на този метод за идентификация е нормално да се анализира, до колко надежден е той. Двата фактора: „нещо, което знае“ и „нещо, което притежава“ са основни за функционирането на метода и дори „пробив“ на един от двата би довело до понижаване на нивото на сигурност и излагане на риск. Логично е да се запитаме, какво би станало, ако факторът „нещо, което се знае“ е известен и на трета страна и дали е възможно това да бъде избегнато. Към момента, с оглед на съществуващите технологии, може да се каже, че би било трудно да се запази в тайна потребителско име и парола. Дори и web приложението да следва всички правила за сигурност, потребителското име и паролата могат да бъдат „прихванати“ от локалната машина, която се използва за достъп до приложението.

С цел повишаване на сигурността при процеса на идентификация в две стъпки и решавайки гореспоменатия проблем, може да модифицираме методът, като заменим „нещо, което знае“ с „нещо, което притежава“. По този начин методът за удостоверяване на самоличност ще използва два фактора „нещо, което притежава“, като и двата фактора са асоциирани с потребителя на системата. Това от своя страна елиминира възможността за „изтичане“ на информация от типа „нещо, което знае“, понеже такава няма да бъде използвана. Модификацията на метода предвижда по-високи ниво на сигурност, понеже шансът за достъп до двата белега за идентификация на трета страна, по едно и също време, е сравнително по-малък.

За реализиране на модификацията бе избрана RFID (Radio frequency identification) технология. При RFID се използва чип, който при определен радио сигнал предава заключена в него информация – т.н. таг. Всеки таг е уникален и не може да бъде променян или копиран [2]. RFID чиповете са миниатюрен размер и

успешно се вграждат в карти, гривни и др. Прочитането на информацията от RFID чипът става безконтактно от четец, което го прави удобен за използване. Изборът на RFID технологията за реализиране на проекта се подкрепя и от факта, че цената на тези технологии е сравнително ниска.

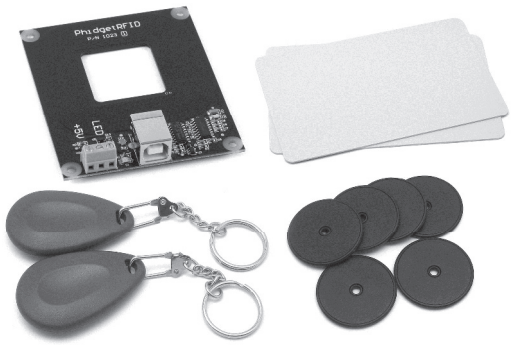
След модифициране, методът за идентификация протича по следния начин: потребителят на web приложението удостоверява своята самоличност посредством лична RFID карта; системата изпраща на потребителя код чрез кратко текстово съобщение – SMS; потребителят въвежда получения код и при съвпадение, получава достъп до системните ресурси.

Създаване на web приложение за удостоверяване на самоличност в две стъпки, използвайки RFID и SMS технологии

Създаването на работещо приложение ще позволи практическо използване на разработения метод, както и провеждане на тестове и интегриране с други системи. Някои от търсените характеристики по време на проектирането на софтуера са: придържане към MVC модела, преизползваемост на софтуерни компоненти, създаване на интуитивен и „приятелски“ графичен интерфейс. Също така при проектирането на приложението са взети под внимание и някои от следните ограничения: програмиране на хардуерни компоненти – интегриране с SMS и RFID модули, интегриране с SMS сървър. След анализ на изискванията и ограниченията към продукта, са взети редица решения свързани с изграждането му. Те са разделени в няколко категории, според характера им, и са описани в следващите подточки.

Използвани хардуерни компоненти

По време на реализацията на проекта са използвани два основни хардуерни модула, отговарящи съответно за обработката на RFID информация и изпращане на SMS съобщения. На фигура 2 е представен RFID на Phidgets.



Фигура 2. RFID четец и чипове

RFID четецът отговаря за разкодиране на информацията във всеки чип и предаването ѝ за обработка към системата. Работната честота на RFID антената е между 125 kHz и 140 kHz. Протоколът, използван за разпознаване на чипове е EM4102, което означава, че всички чипове, използващи този протокол, могат да бъдат използвани в разработваната система. Интерфейсът на четецът е USB 2.0.

Друг, използван, хардуерен компонент е модулът за изпращане на текстови съобщения – фигура 3.

Фигура 3. SMS модул Wavecom Fastrack

Това е програмно управляван модул, симулиращ мобилен телефон. Устройството използва SIM карта, чрез която може да изпраща и получава текстови съобщения. В приложението се използва за изпращане на код за сигурност до потребителите на системата. SMS модулът се свързва посредством сериен порт. За управление на устройството е необходим SMS сървър, в който се конфигурират параметрите на съобщението и който се интегрира с разработеното приложение. За нуждите на проекта е използван SMS сървърът на Ozeki – NG SMS Gateway. Цената на използваните хардуерни компоненти варира в зависимост от някои техни характеристики, но пълният хардуерен комплект, използван в проекта, струва около $150.

Използвани технологии

За реализиране на приложението са използвани различни технологии и приложен софтуер. Изборът на Java, като основен програмен език бе наложен от изискванията към приложението – уеб-базирано, трислойно и с възможност за програмиране на хардуерни компоненти. За постигане на тези цели се използва Java Server Faces – JSF в комбинация с допълнителни библиотеки за подсигуряване на използвания хардуер. За визуалното представяне се използват XHTML в комбинация с Ajax, JavaScript и CSS. За съхранение на информация се използва релационна база от дани. В проекта се използва MySQL база от данни, поддържана от SQL сървър. Заявките към базата данни се генерират автоматично с помощта на Java Persistence API – JPA. Системата е разположена на JBoss Application Server. С цел осигуряване на базова защита се използва JAAS – Java Authentication and Authorization Service.

ЗАКЛЮЧЕНИЕ

Представеният метод за удостоверяване на самоличност от две стъпки помага за повишаване на сигурността при работа с уеб-базирани системи. Методът заменя стандартното използване на потребителско име и парола в процеса на идентификация с персонализирана RFID чип-карта. Това решава редица проблеми свързани с надежността на паролите и начините, по които се съхраняват. На база на разработения метод е създадено уеб-базирано приложение, позволяващо удостоверяване на самоличност посредством RFID и SMS технология. Създаденото приложение се придържа към MVC моделът и използва допълнителни хардуерни компоненти. Разработеното приложение може да бъде интегрирано във вече съществуващи системи за сигурност.

ЛИТЕРАТУРА

[1] Kim,J., S.Hong. A Method of Risk Assessment for Multi-Factor Authentication. Journal of Information Processing Systems, Vol.7, 2011.

[2] Juels,A., RFID security and privacy: a research survey. Selected Areas in Communications, IEEE Journal on (Volume: 24, Issue: 2), 2006

За контакти:

Калоян Миронов, Катедра "Информатика и информационни технологии", Русенски университет "Ангел Кънчев", тел.: 0887 187 148, e-mail: mail@kaloian.net

Докладът е рецензиран.